

COMOMAGINST 5510.1J  
N1

COMOMAG INSTRUCTION 5510.1J

Subj: COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.36  
(b) SECNAVINST 5510.30A  
(c) COMOMAGINST 5530.2A  
(d) COMOMAGINST 1601.1L  
(e) OPNAVINSTINST S5513.7C  
(f) COMOMAG/MOMAGINST 2280.1B  
(g) COMOMAG/MOMAGINST 5230.1C

1. Purpose. To provide Information and Personnel Security guidance specific to Mobile Mine Assembly Group, and to amplify references (a) and (b). This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMOMAGINST 5510.1H.

3. Action. All COMOMAG personnel having access to classified material are directed to comply with applicable sections of references (a) through (g) and this instruction. **Security of classified material is considered an all hands responsibility and is not restricted by clearance level, pay grade or assignment.**

R. E. SWART

Distribution:  
COMOMAGINST 5216.1R  
List I

---

**TABLE OF CONTENTS**


---

<b>Paragraph</b>	<b>Title</b>	<b>Page</b>
<b>CHAPTER 1 - COMMAND INFORMATION AND PERSONNEL SECURITY PROGRAM</b>		
1-1	Program Management	1-1
1-2	COMOMAG Security Organization	1-1
1-3	Emergency Plan	1-3
1-4	Reviews and Inspections	1-3
1-5	Security Education	1-4
1-6	Internal Procedures for Reporting/ Investigating Compromises and other Security Violations	1-4
<b>CHAPTER 2 - CLASSIFICATION MANAGEMENT</b>		
2-1	Classification Management	2-1
2-2	Marking of Classified Material	2-1
2-3	Working Papers	2-1
<b>CHAPTER 3 - ACCOUNTABILITY AND CONTROL</b>		
3-1	Access	3-1
3-2	Safekeeping and Storage	3-1
3-3	Reproduction, Receipt, Destruction and Transmittal	3-2
3-4	Inventories	3-5
<b>CHAPTER 4 - PERSONNEL SECURITY</b>		
4-1	Clearance Eligibility	4-1
4-2	Security Termination Statements	4-1
4-3	Personnel Security Investigations	4-2
4-4	Security Access List	4-2
<b>APPENDIX A - EMERGENCY ACTION PLAN FOR PROTECTION OF CLASSIFIED MATERIAL AT COMOMAG HEADQUARTERS</b>		

**CHAPTER 1 - COMMAND INFORMATION AND PERSONNEL  
SECURITY PROGRAM**

1-1 Program Management

Introduction. The following procedures and policies are to be used in addition to the guidance set by references (a) and (b). Should a conflict arise, guidance given in references (a) and (b) will take priority over any information enclosed in this instruction.

1-2 Command Management and Organization. Per references (a) and (b), the following individuals shall be assigned to perform security-related duties on the staff of COMOMAG:

a. Command Security Manager (CSM). Responsible to the Commanding Officer (CO) for matters relating to the security and management of classified material, and to the Executive Officer for administration of the Information and Personnel Security Program. The CSM shall:

(1) Be appointed in writing and carry out duties as set by reference (a).

(2) Attend the Naval Security Manager Security Course (S-3C-001).

(3) Be identified on all Plans of the Week (POW), organizational charts and command duty rosters.

(4) Oversee all matters relating to security of classified material for the staff, and provide administrative management for subordinate units as needed.

b. Alternate Command Security Manager shall

(1) Be appointed in writing.

(2) Attend the Naval Security Manager Security Course (S-3C-001).

(3) Serve as CSM during incumbent's absence.

c. Top Secret Control Officer (TSCO) shall

(1) Be appointed in writing.

COMOMAGINST 5510.1J

(2) Be responsible to the CSM and perform duties as set in reference (a).

d. Alternate Top Secret Control Officer shall

(1) Be designated in writing.

(2) Serve as Command TSCO during incumbent's absence.

e. Security Clerk/Classified Material Control Clerk. Shall be appointed per reference (a), and will report directly to the CSM.

f. NATO Classified Material Control Officer. Shall be appointed per reference (a), and will report directly to the CSM.

g. STU-III User Representative/Communications Security (COMSEC) Custodian. Shall be appointed per reference (a), and will report directly to the CO concerning management of STU-III's and COMSEC within the command.

h. Information Systems Security Manager (ISSM) shall

(1) Be appointed in writing.

(2) Report directly to the CO on matters concerning the INFOSEC program.

(3) Be responsible to the CSM for the protection of classified information.

(4) Be responsible to the Physical Security Officer for the protection of personnel, equipment, and related resources.

(5) Oversee duties of the Terminal Area Security Officer and Network Security Officer, and provide administrative management in the area of INFOSEC for subordinate units as needed.

j. Physical Security Officer shall

(1) Be appointed in writing.

(2) Report directly to the CO on matters relating to physical security.

(3) Liaison directly with the CSM, ISSM Security Officer, and COMSEC Custodian concerning protection of classified material, equipment and personnel.

(4) Provide administrative management to subordinate commands as needed.

k. Naval Warfare Publication (NWP) Custodian shall

(1) Be appointed in writing.

(2) Ensure administrative control of related publications.

1-3 Emergency Plan and Security Support

a. Per paragraph 2-13 of reference (b), Appendix A outlines the Emergency Action Plan (EAP) for protection of classified material under the control of COMOMAG. Authority is delegated to the Commanding Officer, Naval Air Station Corpus Christi for matters involving search and seizure and granting or denying access to COMOMAG Headquarters.

b. In the interest of maintaining an efficient security program, all personnel are encouraged to keep classified holdings to a minimum. **Department Heads shall conduct an annual review of classified material within their department and forward results to CSM.**

c. To ensure maximum safeguarding of classified material in the event of an emergency requiring immediate evacuation, all security containers will remain closed when not in use and classified material only removed from its container when actually in use.

1-4 Reviews and Inspections

a. Unless otherwise directed by higher authority, general security reviews and inspections of COMOMAG and subordinate units will be accomplished in conjunction with the Quality Review Program. The CSM shall ensure results of the security portion of such reviews or self-assessments are identified and retained on file. Internal security reviews shall be conducted annually.

b. Specific security programs relating to ISSM, COMSEC and NATO classified material shall be reviewed as required by regulations specific to those programs.

COMOMAGINST 5510.1J

1-5 Security Education. The CSM will ensure security training is conducted for all personnel on the staff of COMOMAG on a regular basis. The Training Officer shall maintain records of attendance. Minimum requirements for security education to be arranged by the CSM per paragraph 4-1 of reference (b) include:

- a. Indoctrination - If not already done during access.
- b. Orientation - All hands at time of assignment.
- c. On-the-Job Training - As required by specific duties.
- d. Annual Refresher Briefings - All hands.
- e. Counterespionage Briefings - All hands, bi-annually.
- f. Special Briefings - As required by specific duties.

(1) NATO Briefings - Upon gaining access and termination of access to NATO classified material.

(2) Foreign Travel Briefings - As required by local NCIS field office.

g. Debriefings - As required by paragraph 4-11 of reference (b) and to be done in conjunction with a Security Termination Statement (OPNAV Form 5511/14) by the CSM.

1-6 Internal Procedures for Reporting/Investigating Compromises and Other Security Violations.

a. The daily use of activity security checklists by duty section personnel as prescribed in reference (d) inherently minimizes the likelihood of a serious incident occurring. However, in the event that possible loss or compromise of classified material occurs, specific reporting and investigative steps must be taken per reference (a).

b. The CSM shall be notified immediately in the event of any suspected loss or compromise and shall coordinate with the CO and XO concerning reporting, investigating and coordination with other agencies, such as NCIS.

c. If a classified material security container is found open and unattended, or classified material is left unattended, the following actions will be taken:

(1) The person making the discovery shall ensure the material or container is safeguarded until properly relieved by another competent and cleared individual.

(2) The Staff Duty Officer (SDO) will be informed immediately.

(3) The SDO will inspect the scene, determine the accountable custodian or sub-custodian, initiate recall of that person and inform the CSM, cognizant department head and XO.

(4) A complete inventory of that container will be conducted and a written report of findings will be submitted to the CSM by the custodian/sub-custodian via the responsible department head.

(5) If the discovery involves separate classified material, the custodian/sub-custodian will page check the material to ensure completeness and provide an explanation of the accountability of the material to the CSM via the responsible department head.

d. Suspected Loss or Possible Compromise. Any person having knowledge of suspected loss or possible compromise of classified material will make an immediate report to the CSM who will take appropriate action set in reference (a).

## CHAPTER 2 - CLASSIFICATION MANAGEMENT

### 2-1 Classification Management

1. Classification Designations. Classification designations shall be per reference (a).

2. Original versus Derivative Classification Authority

a. Original classification is the initial determination that information requires, in the interest of national security, protection against unauthorized disclosure and a determination of the level of protection required. Original classification authorities are designated in reference (a). For items involving mine warfare, reference (e) applies; COMINEWARCOM is designated to have original classification authority. COMOMAG does not have original classification authority for any type information.

b. Derivative classification must be accomplished by anyone who incorporates, paraphrases, restates, or otherwise generates in new form, information already classified by an original classification authority. Derivative information must be marked and safeguarded per original classification requirements. Personnel must ensure all sources are consulted and when a conflict in classification exists, the highest classification level must be utilized. Additionally, all sources must be listed and the marking "multiple sources" indicated as applicable when marking information with source data. Reference (a) applies.

c. Declassification and downgrading will be initially screened by Department Heads and requires final approval by the CSM after coordination with appropriate authorities as required.

2-2 Marking of Classified Material. The guidelines of reference (a) will be followed concerning the marking of classified material produced. Questions concerning the marking of material shall be referred to the CSM. Department heads or their designated custodians will review newly generated classified material for correct classification and marking. The CSM will conduct periodic spot checks of classified material produced to ensure proper marking is conducted.

2-3 Working Papers. All working papers will be marked per reference (a) chapter 7-6 and they will contain the identification of the person producing the material and department. Classified notes from training courses or



conferences are also considered working papers and shall be marked accordingly.

2-1

COMOMAGINST 5510.1J

### **CHAPTER 3 - ACCOUNTABILITY AND CONTROL**

General. All hands are responsible for ensuring the security and accountability of classified material in their control at all times. The following guidance to establish general accounting and control procedures. Unique requirements may require additional procedures particular to the information or situation involved. The CSM will be consulted and determine procedures for any unique requirements as required.

**WITHIN ALL SPACES ASSIGNED TO THE COMOMAG HEADQUARTERS STAFF, DESKS ARE NOT CONSIDERED AS PROPER STORAGE CONTAINERS FOR THE STORAGE OF CLASSIFIED MATERIAL AND WILL NOT BE UTILIZED AS SUCH.**

#### 3-1 Access

a. Access to classified material will be limited to personnel who maintain appropriate security clearance and the need to know. Physical security and restricted areas will be maintained per reference (b).

b. The CSM shall maintain and regularly publish a listing of all personnel assigned to COMOMAG and their corresponding security clearances access levels and basis for clearances. Department heads shall ensure personnel maintain appropriate clearance for access to material within their control.

c. Lecturers shall ensure all personnel present maintain appropriate clearances for the classification level of the subject presented by verifying current visitor clearance data has been received by the CSM from corresponding commands as required.

d. The CSM shall ensure a file of all visitor clearance data is maintained on the Quarterdeck. Department heads will approve all after-hours access to classified material in their control. Personnel requiring access to classified material after hours will be logged into the command log including time, rank/rate, name, subject of classified material being worked on, and time work completed.

#### 3-2 Safekeeping and Storage

a. All classified material will be stored in appropriate security containers and all security containers will be locked when not in use. The CSM shall approve all security containers

for use in storing classified material per guidelines of reference (a).

3-1

COMOMAGINST 5510.1J

b. Department heads shall ensure only approved security containers are utilized to store classified material within their control, only authorized personnel have access and that access is recorded on GSA Form 95's.

c. Department will also ensure combinations of security containers are changed as required per reference (a) and all changes are coordinated with the CSM and recorded on GSA Standard Form 700's.

d. The CSM shall conduct random inspections to ensure combinations have been changed as required and access is controlled as required.

e. Department heads shall ensure Part I of Security Container Information Card (Standard Form 700) and a Security Container Check Sheet (Standard Form 702) are maintained for each security container within their control.

f. The CSM, in conjunction with the SWO, shall maintain a file of sealed Part II's of Standard Form 700's for all command security containers on the Quarterdeck for emergency access. The forms will be marked with priority for safeguarding and/or destruction as follows:

(1) Priority ONE - "Top Secret"

(2) Priority TWO - "Secret"

(3) Priority THREE - "Confidential"

g. SDO's shall approve emergency access as required and ensure the XO, CSM and appropriate department head are informed immediately any time emergency access is required.

h. Department heads shall ensure departmental security checks are conducted at the end of each workday and documented utilizing an "Activity Security Checklist" (GSA Standard Form 701).

i. SDO's shall ensure security checks are conducted and recorded utilizing an "Activity Security Checklist" per reference (d).

3-3 Reproduction, Receipt, Destruction and Transmittal

a. Reproduction. Reproduction of classified material shall be kept to a minimum and shall be performed only on systems

3-2

COMOMAGINST 5510.1J

cleared for the appropriate level of information being processed. The CSM, in conjunction with the ISSM Officer, shall designate all copiers and computerized printers with the highest level of classification they are cleared to process. Printers and copiers utilizing film-type rollers must have films properly secured when not in use as once utilized to copy classified, will retain residual information.

b. Copiers and printers utilizing rollers will have five blank copies run following reproduction of material to clear classified information. The Top Secret Control Officer shall coordinate all requests for reproduction of "Top Secret." In addition to requirements of reference (a), the CO will approve all requests for reproduction of "Top Secret" material.

(1) Designation of copiers:

(a) Operations Copier -- Confidential

(b) Minefield Planning -- Secret

(c) Admin -- Confidential

(d) Supply -- Confidential

c. Receipt. Acknowledgement of receipt is required for Top Secret and Secret information transmitted or transported in and out of the command and for all classified information provided to a foreign government. Reference (a) refers.

d. Destruction

(1) Top Secret, Secret, and Confidential correspondence plus classified waste material such as handwritten notes, carbon paper, typewriter ribbon, correspondence, messages, etc., which contain official information, must be destroyed by shredding.

(2) The CSM will establish at least one day each year as a "clean-out day when specific attention and effort are focused on disposition of unneeded classified and controlled unclassified information. "Top Secret" material will be destroyed per reference (a).

(3) The CSM shall designate the highest levels of classification for which shredders are authorized. Department

heads shall ensure compliance with restrictions on shredders. Burn bags shall be turned into the command Information System Technician (IT) for destruction.

3-3

COMOMAGINST 5510.1J

e. Transmittal

(1) Mail. All "Secret" and above classified material to be mailed shall be processed by the Administrative Office per reference (a). The Admin Office will prepare all transmittal paperwork and complete the registered mail log for "Secret" material sent with the assistance of the Mail Petty Officer. The Admin Office will maintain a file of return receipts for "Secret" material and notify the CSM whenever receipts fail to be returned. The Assist Admin Officer will monitor the packaging of all classified material to ensure requirements of reference (a) are met at all times.

(2) Messages. Processing of outgoing "Top Secret" messages shall be limited to the command IT computer directory.

(3) Classified FAXs. Outgoing classified FAX's shall be sent by secure FAX/STU-III.

(4) Hand Carrying. Personnel delivering classified material locally by hand carrying shall ensure the requirements of reference (a) are fulfilled and that appropriate paperwork is completed as directed by the SC/CMCC. Travelers authorized to hand-carry classified material by the CSM shall ensure material in their possession is afforded appropriate safeguards enroute as required and that if to be turned over to destination command, all required paperwork is returned to COMOMAG as required.

(5) STU-III Voice and Communications Security

(a) Regular, unsecured telephone lines will be answered as follows: "Commanding Officer, Mobile Mine Assembly Group, this is a non-secure line, receptionist's rank/rate and name, may I help you."

(b) Secure STU-III lines will be utilized to discuss any classified, or sensitive, information. No attempt shall be made to "talk around" classified information. STU-III's shall be managed per reference (f).

(6) Cover Sheets and Standard Labels. Classified material removed from storage shall be kept folders with appropriate cover sheets (GSA Standard Forms 703, 704, and 705) when at all possible for ready identification. Removable classified IS media (i.e. removable hard drives and diskettes),

will be marked with Standard Labels 706, 707, 708, 709, 710 and 711 as appropriate.

3-4

COMOMAGINST 5510.1J

(7) Working Papers. All working papers shall be marked with rank/rate and name of creator and department in addition to requirements of reference (a). Working papers shall not normally be kept more than six months without being brought under permanent control. Classified notes from training courses or conferences are also considered working papers and shall be controlled accordingly.

3-4 Inventories. Inventories shall be conducted per reference (a) as a minimum. Each Department Head is required to conduct an annual inventory of all Secret and above material for which they are accountable. Inventories of IS materials will be per reference (g) and, if kept in a security container, the container inventory will include a copy of the IS inventory as well.

## **CHAPTER 4 - PERSONNEL SECURITY**

### **4-1 Clearance Eligibility**

a. Any having knowledge concerning information which may effect an individual's reliability and trustworthiness in maintaining security clearance eligibility is required to inform the CO, XO or CSM. Personnel are cautioned that situations as described in Chapter 8 of reference (b) may adversely effect their ability to retain security clearance eligibility. The following actions will be taken by the CSM in these instances:

(1) The CSM will report adverse information to DON CAF, as required by reference (b), and take other command action as deemed necessary. Upon arrival at COMOMAG, department heads will recommend personnel for access to appropriate level of classification based on "need to know."

(2) The CSM will conduct a review of the individual's records for potentially adverse information and appropriate documentation on member's OPNAV Form 5520/20.

(3) The CSM will ensure documentation of classified information Non-Disclosure Agreement (NDA) (Form SF 189/189A or 312) on member's Form 5520/20 prior to granting clearance or access. If not annotated, the CSM will complete form with the member, ensure annotation on Form 5520/20 and ensure the form is processed as required by reference (b).

b. Favorable Determinations. If no adverse information and proper documentation of pre-requisite investigative requirements exists, the CSM will grant member temporary clearance and coordinate final clearance with DON CAF.

c. Unfavorable Determinations. Should adverse information exist, the CO, in conjunction with the XO, CSM and department head shall determine if security clearances will be withheld. The CSM will ensure all requirements of references (a) and (b) are fulfilled with the assistance of the Legal Officer and DON CAF as required.

4-2 Security Termination Statements. The CSM shall administer all Security Termination Statements as required by reference (b).

The Administrative Department will retain a copy in command files.

4-1

COMOMAGINST 5510.1J

4-3 Personnel Security Investigations. Shall be coordinated and screened for accuracy and completeness by the CSM per reference (b). All personnel subject to a personnel security investigation are required to provide accurate required documentation in a timely manner to maintain eligibility for continued security clearance.

4-4 Security Access List. The CSM shall maintain and publish a command security access list, with the assistance of the N6 Department reflecting all personnel assigned, rank/rate, social security number, clearance, type and date of basis, and investigative authority. A current copy of this listing will be maintained for reference by all department heads and on the Quarterdeck at all times.

**APPENDIX A**  
**EMERGENCY ACTION PLAN FOR PROTECTION OF CLASSIFIED MATERIAL**  
**AT COMOMAG HEADQUARTERS**

1. Activation Authorization. The following personnel are authorized to determine if an emergency condition exists and initiate implementation of this emergency plan, or portions thereof, as required:

- a. Executive Officer
- b. Staff Duty Officer
- c. Command Security Manager
- d. Physical Security Officer
- e. ISSM Officer

The CO, XO and CSM shall be notified immediately whenever this plan is activated and of which portions are activated.

2. Identification of Material. Within the headquarters staff organization of COMOMAG, classified material (Secret and above) is held in the following departments and includes the listed types:

a. Administrative Department - Documents and computer hard drives.

b. Operations Department - Documents, safes and computer hard drives.

c. Supply Department - Computer hard drives

d. Mine Field Planning Department - Documents, safes and computer hard drives.

e. AIS Department - Documents, safes and computer hard drives.

f. Training Department - Documents, computer hard drives and audio-visual products.



- d. Quarterdeck - Computer hard drive.

COMOMAGINST 5510.1J

3. Vulnerability Assessment. As part of the assessment, each incident which occurs must be evaluated for time urgency and responses adjusted accordingly to minimize and prevent loss of life or injury to personnel yet provide maximum security. The following general vulnerability assessment is provided for the potential local conditions that may erupt into emergency situations:

- a. Fire/Bomb Threats/Natural Gas Leaks - Moderate risk.
- b. Civil Disturbance - Low risk.
- c. Enemy Action - Low risk.
- d. Earthquakes - Moderate risk.
- e. No-Notice Severe Inclement Weather (i.e., tornadoes)  
- Moderate risk.
- f. Advance-Notice Inclement Weather (i.e., hurricanes)  
- Moderate risk.

4. Resources and Personnel

a. Reference (c) details the physical security plan for COMOMAG. Commanding Officer, Naval Air Station Corpus Christi has been delegated authority for matters involving search and seizure and the granting or denying of access to the Naval Air Station where COMOMAG is located.

b. Base Security provides the primary response units for matters involving physical security and Fire Department provides the primary fire response. Additional assistance may also be requested from NAS as required. As COMOMAG Staff does not include a formally trained security force, the assistance of Base Security shall be summoned immediately should an unauthorized individual be discovered by any person at COMOMAG attempting to, or actually gaining access to classified material within the control of COMOMAG.

c. All personnel on the staff of COMOMAG shall assist in the implementation of emergency security procedures as required,

including immediate recall if deemed necessary by competent authority.

## 5. Actions

a. The CSM, working in conjunction with the CO and XO, shall determine what, if any, permanent changes to the command security program or other action is deemed necessary following implementation of this EAP. The purpose of this plan is to develop standardized temporary actions to safeguard classified material in the event of an emergency. As circumstances widely vary with each emergency and guidance particular to a situation may be promulgated from higher authorities at any time, flexibility may be required.

b. The CSM shall determine additional alternate actions and ensure compliance with further direction as required. The following priorities apply to the protection of classified material:

- (1) Priority ONE - Top Secret
- (2) Priority TWO - Secret
- (3) Priority THREE - Confidential.

c. The following general categories of actions of a temporary nature apply and shall be initiated by personnel authorized in paragraph (1) above, or by the most senior person present if none of the above are available, based on this plan:

(1) On-site Action. The following actions enable the highest level of protection of classified material utilizing only COMOMAG facilities:

(a) In the event that evacuation of the building due to threats to personnel, i.e., risk of injury or death apply such in the case of fire, bomb threat or natural gas leak, securing classified material shall not take precedence over safe evacuation. Personnel shall evacuate the building immediately as per established fire evacuation procedures. Prior to evacuation, priority will be on securing as many security containers and greatest amount of material at highest classification as possible without delaying evacuation unduly.

(b) Following evacuation and muster, the SDO shall coordinate with the CSM or other security personnel listed in paragraph (1) above to ensure the building is secured and access is limited. Guards at entrances shall be posted as necessary, maintaining the safety of personnel at all times. Each

COMOMAGINST 5510.1J

department head shall survey their personnel to determine what classified material and/or containers have been left unsecured, if any. Following completion of the evacuation, department heads shall ensure their personnel review their areas to determine what effect on classified material has occurred and report findings to the CSM.

(c) In the event of any emergency allowing advanced warning (i.e., the onset of a hurricane following days of tracking or gradual build-up of the threat of enemy action, etc.), maximized storage of classified material will be in the command vault. Vault storage will be limited to only classified material.

(d) To the maximum extent possible, security containers will be moved into the vault with an emphasis on those containing the highest level of classification. As the vault is in itself a security container, material classified as "Confidential" may be stored in sealed boxes inside the vault if space becomes limited.

(e) If prolonged storage and access to material required, boxes are not required to be sealed. All boxes will be marked on the outside with classification level and cognizant department.

b. In-area action. In conjunction with steps listed above, the facilities at COMINELWARCOM may also be utilized. As COMINELWARCOM does not have excess security containers, all classified material from COMOMAG must be retained in its corresponding security container.

c. Out-of-Area Action. This action would entail mailing or shipping classified material to an area outside of Corpus Christi, TX for safekeeping. The CSM, in conjunction with department heads and the CO and XO, shall ensure material holdings are minimized. The CSM shall then coordinate the mailing or shipping of material per reference (a) with the assistance of the Supply Officer. The destination site shall be COMINELWARCOM, or as otherwise determined by circumstances, as arranged by the CSM at the time of the emergency.

d. Destruction

(1) In the event it is determined that classified material cannot be properly safeguarded during an emergent

situation, those personnel identified as activation authorities in paragraph (1) above may direct emergency destruction of classified material.

(2) Destruction shall be conducted to ensure emergent approved methods as described in reference (a) are utilized. Every attempt will be made to maintain an inventory of material destroyed for later accountability determination. However, undue time shall not be spent during destruction so as it put the safeguarding of material or personnel at risk. The person authorizing the destruction shall submit inventories to the CSM at the first opportunity following the situation.

